UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/704,790	11/03/2000	Walter Mason Stewart	109993.00103	7495

27557 7590 10/23/2003

BLANK ROME LLP
600 NEW HAMPSHIRE AVENUE, N.W.
WASHINGTON, DC 20037

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2131	14

DATE MAILED: 10/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/704,790	STEWART ET AL.	
	Examiner	Art Unit	
	Paula W Klimach	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 August 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☒ Claim(s) *42 and 43* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This office action is in response to amendment filed on 8/12/03 (Paper No. 13). Original application contained Claims 1-43. Applicant amended Claims 1, 16, and 31. The amendment filed on 8/12/03 have been entered and made of record. Therefore, presently pending claims are 1-43.

Response to Arguments

2. Applicant's arguments filed 8/12/03 have been fully considered but they are not persuasive because of following reasons.

3. Applicant argued, "*Kellum emphasizes a signal-level process that operates below the software layer of a system (see, e.g., column 11, paragraph beginning at line 32). Examples of such a signal-level process include the use of a television card or a facsimile machine. In other words, Kellum fails to teach or suggest application-level conversion and in fact teaches away from it.*" This is not found persuasive. Kellum does not teach away from software layer (column 2 lines 31-36), but instead teaches enhancing the software layer. Kellum teaches in column 6 lines 14-23, that the preferred method of operation of the prior art is in the software level and therefore virus detection in the software level is well known. Kellum's system is an improvement to the prior art as Kellum indicates in column 6 lines 7-10, that the software based systems must be in an error free and complex environment to enforce a security policy. The system disclosed by Kellum further receives the data at the signal level and then carries out the operations of all the levels above that, which include the application level such as file updates (column 4 lines 49-59).

4. In reference to applicant's argument regarding claims 1, 16, and 31, "*Kellum describes what is essentially a unidirectional signal-level conversion from one data transport format to another. Any semantics of the data and its interpretation by a human or machine recipient are not considered. Specifically, the transformation from one transport mechanism to another is not intelligent. It relies on attributes inherent in the transport media to retain or discard information, rather than relying on an active computational process to interpret the data and remove unauthorized code or repurpose it into a safe form.*" This is not persuasive since the applicant claims the "converting the email message from an executable format to a non-executable format." The reference teaches the conversion of the message from an executable format to a non-executable format (claim 1 lines 14-18).

5. In reference to the applicant's argument, "*the application-level conversion of the present claimed invention retains the original human-readable semantic content.*" This is not persuasive because Kellum preserves the information and therefore human-readable semantic content (column 7 lines 45-47).

6. In reference to the applicant's argument, "*the present claimed invention uses one of a plurality of software-level conversion processes selected in accordance with a type of the e-mail message.*" The applicant claims that the type of conversion process that is selected is in accordance with a type of e-mail message. Kellum suggests that the process of conversion is also in accordance with the type of email in his description of the transport/recovery transformation pair (column 11 lines 11-25).

7. Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to teach the

invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that Kellum does teach or suggest the subject matter broadly recited in independent Claims 1, 16, and 31. Dependent Claims 2-15, 17-30, and 32-43 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action (Paper No. 14). Accordingly, rejections for claims 1-41 are respectfully maintained.

Claim Objections

Claim 1 objected to because of the following informalities: claim reads, "virus c ontained in an e-mail" on line 1, should read "virus contained in an e-mail". Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The applicant's argument on the amendment files 8/12/02 is persuasive therefore the rejection under 112 (office action paper 12 filed 5/21/02) has been withdrawn.

Claim Rejections - 35 USC § 102

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

9. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. **Claims 1, 16, and 31** are rejected under 35 U.S.C. 102(e) as being anticipated by Kellum (6, 487, 664) and the Microsoft Computer Dictionary.

Kellum describes a method for protecting a network, claim 1 lines 1-3. The Kellum system protects the network from hostile data (viruses), contained in the information exchange between a protected network and the external information source, claim 1 lines 1-11. An email message is a form of information, in the form of text messages and computer files, which is exchanged over a computer network, Microsoft Computer Dictionary page 173. The Kellum system receives the messages through an intermediate computer hardware device IDS 12, fig. 2, claim 1 lines 8 and 9. The intermediate domain screen IDS serves as a gatekeeper server. Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. The Kellum system chooses from a plurality of conversion processes, column 9 lines 56-60. Furthermore, the Kellum system also maintains the appearance, human readability and semantic content of the email, by creating a second format that contains the information from the first format, claim 1 lines 16-18. Finally the Kellum system sends the email to the recipient, claim 1 lines 19-22.

Furthermore, Kellum disclose a system that chooses from a plurality of processes selected in accordance with the type of email, column 11 lines 11-25. In this section of the specification Kellum indicates that the type of transformation of the first format to the second format depends on the format of the incoming signal.

Claim Rejections - 35 USC § 103

11. **Claims 2 and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum as applied to claims 1 and 16 respectively above, and further in view of Cornetto et al.

Kellum does not describe executable code embedded email as files that can contain viruses.

Cornetto teaches of HTML formatted email, which acts like a browser, page 1 paragraph 4 and 5.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to receive the email Kellum's virus elimination system, run the HTML formatted email, the executables within the email as described by Cornetto (page 2 paragraph 1), in the intermediate domain device before, it is sent to another user. One of ordinary skill in the art would have been motivated to do this because embedded executables run locally and if they contain malicious scripts they could create disruptive virus behavior, Cornetto page 2 paragraph 1.

12. **Claims 3 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and Cornetto, as applied to claim 2, and 17 respectively above, and further in view of Allen (5940614) and Brown.

Allen discloses a system that can deactivate and reactivate hyperlinks to provide a hypertext control method and apparatus in which different hypertext information or different target modules are displayed based upon a user class or authority, column 2 lines 2-6.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to receive in the intermediate domain device as described by Kellum, and

deactivate hyperlinks as in Allen. One of ordinary skill in the art would have been motivated to do this because clicking on hyperlinks in email can lead to virus infection, Brown paragraph 20.

13. **Claims 4, 5, 20 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of Kellum.

In reference to claim 4 and 19, Brown teaches that executable files attached to e-mail could cause a virus to infect a computer, page 2 paragraph 1.

Brown does not teach of a system to protect the network against the fore mentioned viruses.

Kellum describes a method for protecting a network, claim 1 lines 1-3. The Kellum system protects the network from hostile data (viruses), contained in the information exchange between a protected network and the external information source, claim 1 lines 1-11.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the Kellum network protection system on the email described by Brown. One of ordinary skill in the art would have been motivated to do this because universal protection of information is needed, whereby protection is easily verifiable, cost-effective, and does not require prior knowledge to successfully execute a detection, Kellum column 2 lines 31-35.

In reference to claims 5 and 20, Kellum further teaches of the intermediate domain device being made up of sockets, which connect the IDD to the external system, column 2 lines 46 and 47. These sockets perform the task of the gatekeeper, column 6 lines 40-48. The socket sends these signals to the sacrificial server (the intermediate domain device IDD), Fig. 2. The IDD

then converts executable files into non-executable files during the modified read claim 1 lines 14-18.

14. **Claims 6, 7, 21, 22, 32, and 33** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and Brown as applied to claims 4, 16, and 31 above, and further in view of Schnurrer et al (5,842,002).

In reference to claim 6, 21, and 32, Kellum and Brown do not expressly disclose looking for virus activity.

Schnurer discloses a system that looks for computer virus activity which include changes in the IRQ table, FAT, and files, Fig. 6C.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to look for virus activity in server 20. One of ordinary skill in the art would have been motivated to do this because virus activity indicates the presence of a virus in the network, Schnurer column 7 lines 53-67.

In reference to claim 7, 22, and 33, Kellum discloses a system where in the case of contamination of the IDS from hostile code the IDS can be rebooted safely from a safe copy of the operating system, column 4 lines 39-42.

15. **Claims 8 and 23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and Brown as applied to claims 5 and 20 respectively above, and further in view of Swift et al (6,377,691 B1).

Kellum and Brown do not disclose a method wherein communication between the gatekeeper server and the sacrificial server is authenticated using a challenge-and-response technique.

Swift discloses a system that uses a challenge-response authentication technique to authenticate the communication between a client and server, abstract.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a challenge-response authentication technique to authenticate the sacrificial server, 20. One of ordinary skill in the art would have been motivated to do this because the challenge-response authentication technique prevents the replay of messages therefore detecting intruders, Swift column 3 lines 19-21 and column 3 lines 44-46.

16. **Claim 34** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and the Microsoft dictionary as applied to claim 31 above, and further in view of Swift.

Kellum does not disclose a method wherein communication between the gatekeeper server and the sacrificial server is authenticated using a challenge-and-response technique.

Swift discloses a system that uses a challenge-response authentication technique to authenticate the communication between a client and server, abstract.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a challenge-response authentication technique to authenticate the sacrificial server, 20. One of ordinary skill in the art would have been motivated to do this because the challenge-response authentication technique prevents the replay of messages therefore detecting intruders, Swift column 3 lines 19-21 and column 3 lines 44-46.

17. **Claims 9, 24, and 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown and Kellum as applied to claims 4, 16, and 31 respectively above, and further in view of Ji et al (5,623,600) and Battersby et al (5,740,370).

Brown and Kellum do not disclose a system that maintains a list of approved attachment types.

Battersby discloses a system that maintains a list of file type identifiers in order to determine whether a file belongs to a certain file subset of files, column 14 lines 18-25.

Ji discloses a system that determines whether the attachment is of a type, which is in the list of approved attachments types (types that do not contain viruses), fig 6B. Ji also sends a virus detection message to the client as a reply, fig 6B.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a list of approved attachment types in server 20, determine whether the attachment is a type which is in the list described by Battersby with the method described by Ji, and inform the recipient that a message containing a non-approved attachment has been received, as described by Ji. One of ordinary skill in the art would have been motivated to do this because it would not affect the performance of individual computers, Ji column 2 lines 23-30.

18. **Claims 10, 25, and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and the Microsoft Computer dictionary as applied to claims 1, 16, and 31 respectively above, and further in view of Ji et al (5,623,600) and Jury et al (5,618,054).

Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18.

Kellum does not disclose a system that maintains a list of approved executable code.

Jury discloses a process that maintains a list of files retrieved by the user in order to delete the files when the user terminates the Electronic Performance Support System, column 10 lines 17-22.

Ji discloses a system that determines whether the attachment is of a type, which is in the list of approved attachments types (types that do not contain viruses), fig 6B. Ji also sends a virus detection message to the client as a reply, fig 6B. The types of files that are suspected virus carriers are executable code, column 7 lines 33-40.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a list of approved executable code as described by Jury, determine whether the attachment is executable code in the list of executable code as in Ji, and deactivate the executable code if it is not in the list, as described by Kellum. One of ordinary skill in the art would have been motivated to do this because maintaining a list of files gives the user a choice of files to deactivate, Jury as shown in column 7 lines 32-38.

19. **Claims 11, 12, 13, 26, 27, 28, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum, Microsoft Computer dictionary, Ji, and Jury as applied to claims 10, 25, and 36 above, and further in view of Corthell (6,192,477 B1), Horwitt, and Rad.

In reference to claim 11, 12, 26, 27, and 28, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Ji and Jury do not disclose a method for determining whether the executable code has been altered, using an check-summing algorithmic technique.

Corthell discloses a system that uses the checksum algorithm to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered using the method of Corthell, using an algorithm. Then deactivate the executable code if it has been altered using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common way to check if files have been altered, Horwitt, abstract.

In reference to claim 13, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Ji, and Jury do not disclose a method for determining whether the executable code has been altered, using a check-summing algorithmic technique.

Corthell discloses a system that uses the checksum to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a checksum algorithm as shown in Corthell. Then deactivate the executable code if it has been altered using

the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common algorithm of checking the corruption of files, Horwitt, abstract. If the file has been corrupted (altered), it is possible that it contains a virus, Rad, paragraphs 13-16 and 30.

In reference to 37, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Ji and Jury do not disclose server for determining whether the executable code has been altered, using an check-summing algorithmic technique.

Corthell discloses a system that uses the checksum algorithm to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a checksum algorithm, as shown by Corthell. Then deactivate the executable code if it has been altered, using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common algorithm of checking the corruption of files, Horwitt, abstract. If the file has been corrupted (altered), it is possible that it contains a virus, Rad, paragraphs 13-16nad 30.

20. **Claims 38, and 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum, Brown, and Schnurrer, as applied to claim 32 above, and further in view of Corthell (6,192,477 B1), Horwitt, and Rad.

In reference to 38 and 39, Kellum system also converts the e-mail message from an executable format to a non-executable format, claim 1 lines 14-18. This would deactivate the executable code.

Kellum, Brown, and Schnurrer do not disclose server for determining whether the executable code has been altered, using an check-summing algorithmic technique.

Corthell discloses a system that uses the checksum algorithm to determine whether a file has been altered, column 8 lines 7-16.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a checksum algorithm, as shown by Corthell. Then deactivate the executable code if it has been altered, using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because checksum is a common algorithm of checking the corruption of files, Horwitt, abstract. If the file has been corrupted (altered), it is possible that it contains a virus, Rad, paragraphs 13-16 and 30.

21. **Claims 14, 29, and 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum, Microsoft Computer dictionary, Ji, Jury, Corthell (6,192,477 B1), Horwitt, and Rad. as applied to claims 12, 27, and 38 respectively above, and further in view of Helbig Sr. et al (6,311,273 B1).

Kellum, Microsoft Computer dictionary, Ji, Jury, Corthell (6,192,477 B1), Horwitt, and Rad do not disclose a method that utilizes a hashing function.

Helbig discloses the use of a hashing algorithm to determine if control software has been altered, column 1 lines 57-60.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to determine whether the executable code has been altered, using a hashing algorithm, as shown by Helbig. Then deactivate the executable code if it has been altered, using the method disclosed by Kellum. One of ordinary skill in the art would have been motivated to do this because a hashing function is a secure method of determining that code has not changed and thus that the trusted code has not been altered, column 1 lines 65-68.

22. **Claims 15, 30, and 41** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kellum and the Microsoft Computer dictionary as applied to claims 1, 16, and 31 above, and further in view of Field et al (6, 253, 324).

Kellum does not disclose a method where a copy is make of the executable code, executing the first copy and not the second copy and comparing the effect of the executable code.

Field discloses a system where executable code is stored in an image file and the same code is copied and then executed in and executable image. Then a comparison is made of the non-writeable sections of the executable image and that of the verified image file. If the images match then the client is verified, column 2 lines 30-45.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to make a copy of the executable code in the IDS and run one copy and not the other in order to compare the result of running the code, as disclosed by Field. Then deactivate

the executable code if it has been altered. One of ordinary skill in the art would have been motivated to do this because running one copy of the code and not the other a way to detect attacking programs that modify memory images of legitimate programs in order to alter its execution, column 2, lines 17-27.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK

FRANTZ B. JEAN
PRIMARY EXAMINER